(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 923 062 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
16.06.1999 Bulletin 1999/24

(21) Application number: **98917672.2**

(22) Date of filing: **24.04.1998**

(51) Int. Cl.[6]: **G09C 1/00**, H04L 9/06, G06K 9/00

(86) International application number:
PCT/JP98/01898

(87) International publication number:
WO 98/54687 (03.12.1998 Gazette 1998/48)

(84) Designated Contracting States:
BE CH DE DK ES FI FR GB IT LI NL SE

(30) Priority: **30.05.1997 JP 14132897**

(71) Applicant:
MITSUBISHI DENKI KABUSHIKI KAISHA
Tokyo 100-8310 (JP)

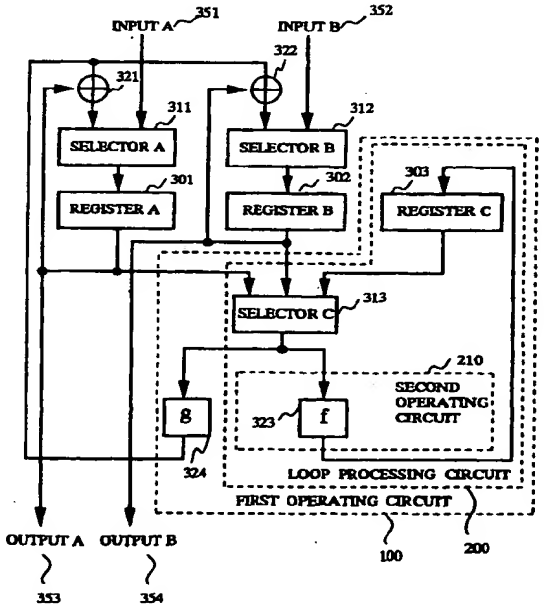
(72) Inventors:
- **MATSUI, Mitsuru,**
  Mitsubishi Denki Kabushiki Kaisha
  Tokyo 100-8310 (JP)
- **TOKITA, Toshio,**
  Mitsubishi Denki Kabushiki Kaisha
  Tokyo 100-8310 (JP)

(74) Representative:
Pfenning, Meinig & Partner
Mozartstrasse 17
80336 München (DE)

(54) CIPHER PROCESSOR, IC CARD AND CIPHER PROCESSING METHOD

(57) The present invention can be applied to a cipher processing apparatus, which includes a function F having a configuration of repeating process and inside of the function F, a function f having a configuration of repeating process is included. According to the invention, the cipher processing apparatus is configured by registers 301 through 303 for temporarily holding data, selectors A through C, 311 through 313, and a function f operating circuit 323 for transforming data. An output data from the function f operating circuit 323 is held in the register C 303, and the selector C 313 selects either to repeat the data transformation by the function operating circuit 323 or not. When a cipher processing apparatus includes a function F having a configuration of repeating process and inside of the function F, a function f having a configuration of repeating process is included, the cipher processing apparatus can be embodied efficiently, which enables to reduce the circuit scale and to save electric power.

Fig. 3



EP 0 923 062 A1

Description

Technical Field

[0001] The present invention relates to a cipher processing apparatus, in particular, to a small-sized cipher processing apparatus installed in an IC (Integrated Circuit) card and so on.

Background Art

[0002] For a conventional related art of the invention, DES (Data Encryption Standard) of U. S. commercially used cipher, which is a block cipher of secret key (common key) cryptosystem, will be explained.

[0003] A detail of DES processing is described in such as Hans Eberl "A High-speed DES implementation for Network Applications", Advances in Cryptology — CRYPTO '92, Lecture Notes in computer Science 740, Springer-Verlag.

[0004] Fig. 18 is a flowchart showing DES encryption algorithm.

[0005] In Fig. 18, reference numerals 1001 — 1004 show operations using function F for data transformation. Reference numerals 1011 — 1014 show XOR operations bit by bit. In the figure, an initial permutation and a final permutation are omitted.

[0006] An operation will be explained.

[0007] An input data 1050 having 2 × n bits (in case of DES, 2 × 32 bits) is divided into two n-bit data 1051 and 1052. The n-bit data 1051 is output as n-bit data 1053 without any transformation. The data 1051 is also input to the function F 1001 to be transformed. The data transformed by the function F 1001 is XORed with the other n-bit data 1052 bit by bit by the XOR operation 1011 and the XORed result is output as n-bit data 1054.

[0008] Hereinafter, operations are repeated by the functions F 1002, 1003, and 1004, the XOR operations 1012, 1013, and 1014 and output data 1055 and 1056 are output. The two n-bit data are united and output as 2n-bit data 1057.

[0009] Fig. 19 shows an example of cipher processing apparatuses performing data transformation similar to the DES encryption as shown in the flowchart of Fig. 18.

[0010] In Fig. 19, reference numerals 1101 and 1102 show registers A and B for holding data. Reference numerals 1103 and 1104 are selectors A and B for selecting one of data. 1105 denotes a function F operating circuit for calculating the function F as data transformation. 1106 denotes an XOR circuit. 1201 and 1202 respectively show n-bit input data A and B. 1203 and 1204 respectively show n-bit output data A and B.

[0011] An operation will be explained.

[0012] An input data having 2 × n bits (in case of DES, 2 × 32 bits) is divided into two n-bit input data A1201 and B1202. The two input data are respectively selected by the selectors A1103 and B1104 and held in the registers A1101 and B1104. The data held in the register A1101 is fed back to the selectors A1103 and B1104 and input to the function F operating circuit 1105 at the same time. After transformed by the function F operating circuit 1105, the data is XORed by the XOR circuit 1106 with the data held in the register B1102. The XORed result is fed back to the selectors A1103 and B1104.

[0013] Next, the selector A1103 selects the XORed result of the XOR circuit 1106, the selector B selects data held in the register A1101, and the registers A1001 and B1002 are respectively updated by these selected data to hold therein. Then, similarly, the operation, corresponding to the operation through the functions F 1002, 1003, 1004 and the XOR circuits 1012, 1013, 1014 shown in Fig. 18, is repeated (looped) a necessary number of times, and the output data A1203 and B1204 are finally output. In case of DES, the operation will be repeated 16 times.

[0014] This conventional related art is described in detail, for example, in Hans Eberl "A High-speed DES Implementation for Network Applications", Advances in Cryptology-CRYPTO '92, Lecture Notes in computer Science 740, Springer-Verlag.

[0015] In a cipher processing apparatus by the above method, when the apparatus is constructed by a plurality of the functions F having similar configuration for processing, it is possible to efficiently construct a processing circuit by using one circuit repeatedly. This enables to reduce the circuit scale and also save electric power. However, there is a problem that when the function F includes a smaller circuit having repeating process, the conventional configuration of the cipher processing apparatus does not efficiently reduce the circuit scale or save electric power.

[0016] The present invention is provided to solve the above-mentioned problem. The invention aims to obtain a cipher processing apparatus, which can be constructed efficiently to reduce a circuit scale and save electric power even if the apparatus has a configuration of repeatedly processing the function F including an internal smaller circuit configured by repeating process.

Disclosure of the Invention

[0017] According to the present invention, in a cipher processing apparatus performing a first data transformation process on an input data a plurality of times by a first operating circuit,

the first operating circuit comprises a loop processing circuit for performing a second data transformation process a plurality of times;
the loop processing circuit comprises a second operating circuit, a data holding circuit, and a selecting circuit to form a processing loop;
the second operating circuit performs the second data transformation process;
the data holding circuit tentatively holds the data on

which the second data transformation process was performed; and
the selecting circuit selects one of to terminate and to continue the second data transformation process by the loop processing circuit.

[0018] The second operating circuit comprises:

a data dividing circuit dividing data input to the second operating circuit into a first divided data and a second divided data;
a third operating circuit transforming the first divided data;
an XOR circuit XORing an output data from the third operating circuit with the second divided data bit by bit; and
a data uniting circuit uniting an output data from the XOR circuit and the second divided data.

[0019] The selecting circuit inputs a data for the first data transformation process by the first operating circuit and a data held in the data holding circuit, and the selecting circuit selects the data held in the data holding circuit when a process by the loop processing circuit is to be continued.

[0020] The selecting circuit selects the data for the first data transformation process by the first operating circuit when a process by the processing loop circuit starts.

[0021] The cipher processing apparatus further comprises:

a register A and a register B alternately holding the data for the first data transformation by the first operating circuit;
two XOR circuits XORing bit by bit the data on which the first data transformation was performed by the first operating circuit with the data held in the register A and with the data held in the register B, respectively;
a selector A and a selector B selecting one of the data on which the first data transformation was performed by a first operating unit and an XORed data by the XOR circuit to hold in the register A and the register B, respectively; and
the selecting circuit alternately selects the register A and the register B to start the process of the loop processing circuit.

[0022] The first operating circuit further performs a data transformation different from the second data transformation process for the data on which the second data transformation was performed by a processing loop unit to output a transformed data.

[0023] The second operating circuit comprises:

m ($m \geqq 1$) number of function operating circuits inputting identical data from the selecting circuit; and
a selector with m inputs and one output for inputting data operated by the m number of function operating circuits and selecting one of the input data.

[0024] The cipher processing apparatus further comprises:

a function operating unit transforming data output from the selecting circuit; and
a selector inputting data operated by the function operating unit and the data output from the selecting circuit, and outputting one of the data.

[0025] According to the present invention, in a cipher processing method performing a first data transformation for an input data a plurality of times by a first operating step,

the first operating step comprises a loop processing step performing a second data transformation at a plurality of times;
the loop processing step comprises:
a second operating step performing the second data transformation;
a data holding step temporarily holding data on which the second data transformation was performed; and
a selecting step for selecting either of to terminate and to continue the second data transformation by the loop processing step.

[0026] The second operating step comprises:

a data dividing step dividing data input to the second operating step into a first divided data and a second divided data;
a third operating step transforming the first divided data;
an XOR step XORing an output data from the third operating step with the second divided data bit by bit; and
a data uniting step uniting an output data from the XOR step and the second divided data.

[0027] According to the present invention, an IC (integrated circuit) card communicating data with a reader/writer comprises:

a data receiving circuit receiving the data from the reader/writer;
a data transmitting circuit transmitting the data to the reader/writer; and
the cipher processing apparatus of the invention encrypting/decrypting the data.

[0028] According to the present invention, an IC card communicating data with a reader/writer comprises:

a data receiving circuit receiving the data from the reader/writer;
a data transmitting circuit transmitting the data to the reader/writer; and
the cipher processing apparatus of the invention encrypting/decrypting the data.

Brief Description of the Drawings

[0029]

Fig. 1 shows an encryption algorithm in relation to a first embodiment of the present invention.
Fig. 2 shows a configuration of a function used for an encryption algorithm in relation to the first embodiment of the present invention.
Fig. 3 is a block diagram showing a basic configuration of a cipher processing apparatus according to the first embodiment of the invention.
Fig. 4 is a flowchart showing one example of basic operations of the cipher processing apparatus according to the first embodiment of the invention.
Fig. 5 is a flowchart showing one example of basic operations of the cipher processing apparatus according to the first embodiment of the invention.
Fig. 6 shows a configuration of the function used for an encryption algorithm in relation to the first embodiment of the present invention.
Fig. 7 shows the encryption algorithm according to the first embodiment of the present invention.
Fig. 8 shows a configuration of the function used for the encryption algorithm according to the first embodiment of the present invention.
Fig. 9 is a block diagram showing a configuration of a second operating circuit according to the first embodiment of the present invention.
Fig. 10 shows an encryption algorithm in relation to a second embodiment of the present invention.
Fig. 11 shows a configuration of a function used for the encryption algorithm according to the second embodiment of the present invention.
Fig. 12 is a block diagram showing a basic configuration of a cipher processing apparatus according to the second embodiment of the invention.
Fig. 13 is a flowchart showing an example of basic operations of the cipher processing apparatus according to the second embodiment of the invention.
Fig. 14 is a flowchart showing one example of basic operations of the cipher processing apparatus according to the second embodiment of the invention.
Fig. 15 is a flowchart showing an example of basic operations of the cipher processing apparatus according to the second embodiment of the invention.
Fig. 16 is a block diagram showing a basic configuration of a communication system according to a third embodiment of the invention.
Fig. 17 is a block diagram showing a basic configuration of an IC according to the third embodiment of the invention.
Fig. 18 shows an encryption algorithm according to the conventional related art.
Fig. 19 is a block diagram showing a basic configuration of a cipher processing apparatus according to the conventional related art.

Best Mode for Carrying out the Invention

Embodiment 1.

[0030] A cipher processing apparatus according to one embodiment of the present invention will be explained referring to Figs. 1 through 3.

[0031] Fig. 1 is a flowchart showing an encryption algorithm of a cipher processing apparatus according to one embodiment of the present invention.

[0032] In Fig. 1, reference numerals 101 through 104 show operations using functions F for data transformation, and reference numerals 111 through 114 show XOR operations bit by bit.

[0033] Fig. 2 shows a configuration of operation using the function F, which is configured by three operations using functions f 201 through 203 and an operation using a function g 211.

[0034] An operation will be described hereinafter.

[0035] An input data 150 having $2 \times n$ bits is divided into two, namely, n-bit data 151 having upper digits of the input data and n-bit data 152 having lower digits of the input data. The n-bit data 151 is output as n-bit data 153 without any transformation, and the n-bit data 151 is also transformed by the function F 101. The output data from the function F 101 is XORed with another n-bit data 152 by the XOR circuit 111 bit by bit and n-bit data 154 is output. In the function F, three operations using the functions f 201 through 203 are performed, an operation using the function g 211 is then performed and the result is output.

[0036] Then, similarly, operations are repeated through the functions F 102, 103, 104, and XOR circuits 112, 113, 114 and n-bit data 155, 156 are output. The two n-bit data are united and output as 2n-bit data 157.

[0037] Fig. 3 shows a general configuration of the cipher processing apparatus embodying the algorithm for data transformation explained by referring to Figs. 1 and 2.

[0038] In Fig. 3, reference numerals 301, 302 and 303 respectively show a register A, a register B and a register C. Reference numerals 311, 312 and 313 respectively show a selector A, a selector B and a selector C. 321 and 322 denote bit by bit XOR circuits. 323 denotes a function f operating circuit, which is one of configurational elements performing the function F operation. 324 denotes a function g operating circuit, which is one of configurational elements performing the function F

operation.

[0039] The register C 303, the selector C 313, the function f operating circuit 323 and the function g operating circuit 324 form a first operating circuit 100. The register C 303, the selector C 313, the function f operating circuit 323 form a loop processing circuit 200.

[0040] Figs. 4 and 5 are flowcharts showing an operation of the circuits shown in Fig. 3.

[0041] The operation will be explained by referring to Figs. 4 and 5.

[0042] The operation by the function F is performed by three-times operation of the function f operating circuit and once operation of the function g operating circuit.

[0043] Data transformation at a first stage shown in Fig. 1 will be explained.

[0044] An input data having $2 \times n$ bits is divided into two n-bit data, namely, an input data A 351 and an input data B 352. The input data are selected by the selector A 311 and the selector B 312, and held in the register A 301 and the register B 302 (at step 4-1).

[0045] Then, in the selector C 313, it is detected whether this is a process of an odd-numbered stage or a process of an even-numbered stage (at step 4-2), the data held in the register A 301 is selected (at step 4-4), and the selected data is transformed by the function f operating circuit 323 (at step 4-6). The output data from the function f operating circuit 323 is held in the register C 303 (at step 4-7). A first operation by the function f operating circuit ends with this step.

[0046] Then, in the selector C 313, the data held in the register C 303 is selected (at step 4-8), and the selected data is transformed by the function f operating circuit 323 (at step 4-6). The data output from the function f operating circuit 323 is held in the register C 303 (at step 4-7). With this step, a second operation by the function f operating circuit ends.

[0047] Further, in the selector C 313, the data held in the register C 303 is selected (at step 4-8). The selected data is transformed by the function f operating circuit 323 (at step 4-6), and the transformed data is held in the register C 303 (at step 4-7). With this step, a third operation by the function f operating circuit 323 ends.

[0048] Next, in the selector C 313, the data held in the register C 303 is selected (at step 4-9). The selected data is transformed by the function g operating circuit 324 and the result is output (at step 4-10). With this step, a whole operation by the function F terminates.

[0049] Next, it is detected whether this is a process of an odd-numbered stage or a process of an even-numbered stage (at step 4-11), the data output from the function g operating circuit 324 is fed back to be XORed with the data held in the register B 302 by the XOR circuit 322 (at step 4-14). The XORed data is selected by the selector B 312 and the selected data is held in the register B 302 (at step 4-15). This step completes the first stage of the data transformation.

[0050] Next, a second stage of the data transformation will be explained.

[0051] It is detected to be an even-numbered stage (at step 4-2), and the selector C 313 selects the data held in the register B 302 (at step 4-3). Then, the selected data is transformed by the function f operating circuit 323 (at step 4-6), and the output data is held in the register C 303 (at step 4-7). A first operation by the function f operating circuit ends with this step.

[0052] Then, in the selector C 313, the data held in the register C 303 is selected (at step 4-8), and the selected data is transformed by the function f operating circuit 323 (at step 4-6). The data output from the function f operating circuit 323 is held in the register C 303 (at step 4-7). With this step, a second operation by the function f operating circuit 323 ends.

[0053] Further, in the selector C 313, the data held in the register C 303 is selected (at step 4-8). The selected data is transformed by the function f operating circuit 323 (at step 4-6), and the transformed data is held in the register C 303 (at step 4-7). With this step, a third operation by the function f operating circuit 323 ends.

[0054] Next, in the selector C 313, the data held in the register C 303 is selected (at step 4-9). The selected data is transformed by the function g operating circuit 324 and the result is output (at step 4-10). With this step, a whole operation by the function F circuit terminates.

[0055] Next, it is detected to be a process of an even-numbered stage (at step 4-11), the data output from the function g operating circuit 324 is fed back to be XORed with the data held in the register A 301 by the XOR circuit 321 (at step 4-12). The XORed data is selected by the selector A 311 and the selected data is held in the register A 301 (at step 4-13). This step completes the second stage of the data transformation.

[0056] Hereinafter, similar processes to the first stage of the data transformation and the second data transformation will be alternately repeated a necessary number of times.

[0057] Finally, the data held in the registers A 301 and B 302 are output as output data A 353 and output data B 354 as a result of the data transformation of the final stage (at step 4-19).

[0058] As has been described, according to this invention, the one function f operating circuit 323 can be used repeatedly by providing the register C 303 and the selector C 313. The cipher processing apparatus does not need to include three function f operating circuits, but need to include only one function f operating circuit 323, which reduces a circuit scale.

[0059] Especially, the function F (the function f, the function g), used for the data transformation for cipher processing, is known to have an extremely complex configuration because the data transformation for cipher processing requires to use a function being strong against cryptanalysis. Hence, the reduction of the circuit scale according to the present invention effects a lot to the data transformation for cipher processing.

[0060] According to the invention, it is not always

required to operate the register A 301, the register B 302, the register C 303, the selector A 311, the selector 312, and the selector C 313. The processes can be performed with these circuits operating only when required, which enables the apparatus to save electric power.

[0061] Accordingly, this invention takes a great effect when applied to a small apparatus such as an IC card. The invention can be applied not only to the IC card, but also to a reader/writer for the IC card.

[0062] The function F is not limited to have the above configuration. For example, when the function F is configured by only repeating the operation of function f as shown in Fig. 6, the function g is not needed for the configuration of Fig. 3. In this case, the data selected by the selector C 313 is directly fed back as shown in Fig. 7.

[0063] When the function f operating circuit 323 includes m ($m \geqq 1$) number of functions, which constitute in an arbitrary order, as shown in Fig. 8, the m number of functions are aligned in parallel at a place corresponding to the function f operating circuit 323 of Fig. 3. The data is input to each of the m number of functions from the selector C 313, the output data from the m number of functions are input to the selector with m number of inputs and one output, and the selector selects one output data to be held in the register C 303 as shown in Fig. 9. These operations are repeated a number of times corresponding to an arbitrary order of the m number of functions.

Embodiment 2.

[0064] A cipher processing apparatus according to another embodiment of the present invention will be explained referring to Figs. 10 through 14.

[0065] Fig. 10 shows a flowchart of MISTY encryption algorithm.

[0066] Details of MISTY is disclosed in, for example, Mitsuru Matsui "Block Encryption Algorithm MISTY", the Institute of Electronics, Information and Communication Engineers, Technical Report ISEC 96-11 (1996-07).

[0067] In Fig. 10, reference numerals 501 through 506 denote operations by functions FL, reference numerals 511 through 514 denote operations by functions FO, and 521 through 524 are XOR operations.

[0068] Fig. 11 shows operations using the functions FO 511 through 514 of Fig. 10.

[0069] As shown in Fig. 11, in MISTY algorithm, transformation process, including functions FI 601 through 603 and XOR operations 611 through 613, is repeated three times as operations by the functions FO 511 through 514.

[0070] Fig. 12 shows one embodiment of a cipher processing apparatus applying the data transformation process of MISTY of Figs. 10 and 11 according to the present invention.

[0071] In the following, an operation of the encryption algorithm of Figs. 10 and 11 will be explained.

[0072] An input data 550 having $2 \times n$ bits is divided into two n-bit data, one having upper n digits of the input data 550 and the other having lower n digits of the input data 550, and the two divided data are input as an input data A 551 and an input data B 552. In case of MISTY, n=32. After transformed by the function FL 501, the n-bit input data 551 is output as n-bit data 553, and is also transformed by the function FO 511. The other n-bit input data 552 is transformed by the function FL 502. The data transformed by the function FO 511 is XORed bit by bit by the XOR operation 521 with the output data from the function FL 502, and n-bit data 554 is output. In the function FO, operations by the functions FI 601 through 603 and the XOR operations 611 through 613 are performed. Namely, the input 2m-bit data (n bits) 650 is divided into two m-bit data 651 and 652. After transformed by the function FI, the data 651 is XORed bit by bit by the XOR operation 611 with the data 652, and the XORed result is output as data 653. The data 652 is output as data 654 without any transformation. Hereinafter, the above operations are repeated in three stages. Finally, two m-bit data are united and output as 2m-bit (n bits) data 655.

[0073] Next, an operation at a second stage will be described.

[0074] The output data 554 supplied from the first stage is output without any transformation, and at the same time, is transformed by the function FO 512. The output data from the function FO 512 is XORed bit by bit by the XOR operation 522 with the other n-bit data 553, and the XORed result is output.

[0075] Hereinafter, data transformation similar to the process of the first and second stages is repeated a necessary number of times, and n-bit data 557 and 558 are output. Finally, the output data is transformed by FL functions 505 and 506 into data, of which the upper digits and the lower digits are exchanged, the two n-bit data are united, and 2n-bit data 559 is output.

[0076] Fig. 12 shows a general configuration of the cipher processing apparatus embodying the data transformation algorithm explained by referring to Figs. 10 and 11.

[0077] In Fig. 12, reference numerals 701, 702, 703 denote a register A, a register B, and a register C, respectively. Reference numerals 711, 712, 713, 714 denote a selector A, a selector B, a selector C, and a selector D. 721, 722, 723 show XOR circuits, 724 shows a function FI operating circuit for data transformation, and 725 shows a function FL operating circuit for data transformation. 751 is an input data A, 752 is an input data B, 753 is an output data A, and 754 is an output data B.

[0078] Here, the register C 703, the selector C 713, the function FI operating circuit 724 and the XOR circuit 723 constitute a first operating circuit 101 for a first data transformation. The register C 703, the selector C 713, the function FI operating circuit 724, and the XOR circuit 723 constitute a loop processing circuit 201.

[0079] Figs. 13 through 15 are flowcharts explaining an operation of the cipher processing apparatus shown in Fig. 12.

[0080] The operation will be described by referring to Figs. 13 through 15.

[0081] First, an input data having 2 × n bits is divided into two n-bit data, and input as an input data A 751 and an input data B 752. In case of MISTY, n=32. The two input data are respectively selected by the selector A 711, the selector B 712 and respectively held in the register A 701, the register B 702 (at step 8-1).

[0082] Next, in the selector C 713, it is detected whether this is a process of an odd-numbered stage or a process of an even-numbered stage (at step 8-2), and the data held in the register A 701 is selected (at step 8-3). Then, the selected data is transformed by the function FL operating circuit 725 (at step 8-4), and the output data is selected by the selector D 714 (at step 8-5). Further, the selected data is selected by the selector A 711 (at step 8-6), and is held in the register A 701 (at step 8-7).

[0083] Next, in the selector C 713, the data held in the register B 702 is selected (at step 8-8). The selected data is transformed by the function FL operating circuit 725 (at step 8-9), and the output data is selected by the selector D 714 (at step 8-10). Further, the selected data is selected by the selector B 712 (at step 8-11), and is held in the register B (at step 8-12).

[0084] Next, in the selector C 713, the data held in the register A 701 is selected (at step 8-13). Then, the selected data (2 × m bits) is divided into two m-bit data, and one m-bit data is output as an output data without any transformation. The other m-bit data is input to the function FI operating circuit 724 to be transformed. The transformed data is XORed bit by bit by the XOR circuit 723 with the other m-bit data, and the XORed result and the output m-bit data are united (at step 8-14). The united output data is held in the register C 703 (at step 8-15). With this step, a first process including the function FI operating circuit 724 has been completed.

[0085] Next, in the selector C 713, the data held in the register C 703 is selected (at step 8-16). The selected data (2 × m bits) is divided into two m-bit data, and one m-bit data is output as an output data without any transformation. The other m-bit data is input to the function FI operating circuit 724 to be transformed. The transformed data is XORed bit by bit by the XOR circuit 723 with the other m-bit data, and the XORed result and the output m-bit data are united (at step 8-14). The united output data is held in the register C 703 (at step 8-15). With this step, a second process including the function FI operating circuit 724 has been completed.

[0086] Next, in the selector C 713, the data held in the register C 703 is selected (at step 8-16). The selected data (2 × m bits) is divided into two m-bit data, and one m-bit data is output as an output data without any transformation. The other m-bit data is input to the function FI operating circuit 724 to be transformed. The transformed data is XORed bit by bit by the XOR circuit 723 with the other m-bit data, and the XORed result and the output m-bit data are united (at step 8-14). The united output data is held in the register C 703 (at step 8-15). With this step, a third process including the function FI operating circuit 724 has been completed.

[0087] Next, in the selector C 713, the data held in the register C 703 is selected (at step 8-16), and the selected data is selected by the selector D 714 (at step 8-18). Then, it is detected whether this is a process of an odd-numbered stage or a process of an even-numbered stage (at step 8-19), the selected data is fed back, and is XORed by the XOR circuit 722 with the data held in the register B 702 (at step 8-20). The output data from the XOR circuit B 702 is selected by the selector B 712 (at step 8-21), and is held in the register B 702 (at step 8-22). With this step, the data transformation process of the first stage terminates.

[0088] Next, a data transformation process corresponding to the data transformation process of the second stage shown in Fig. 10 is performed.

[0089] First, in the selector C 713, it is detected to be an even-numbered stage (at step 8-2), and the data held in the register B 702 is selected (at step 8-24).

[0090] The selected data (2 × m bits) is divided into two m-bit data, and one m-bit data is output as an output data without any transformation. The other m-bit data is input to the function FI operating circuit 724 to be transformed. The transformed data is XORed bit by bit by the XOR circuit 723 with the other m-bit data, and the XORed result and the output m-bit data are united (at step 8-14). The united output data is held in the register C 703 (at step 8-15). With this step, a first process including the function FI operating circuit 724 has been completed.

[0091] Next, in the selector C 713, the data held in the register C 703 is selected (at step 8-16). The selected data (2 × m bits) is divided into two m-bit data, and one m-bit data is output as an output data without any transformation. The other m-bit data is input to the function FI operating circuit 724 to be transformed. The transformed data is XORed bit by bit by the XOR circuit 723 with the other m-bit data, and the XORed result and the output m-bit data are united (at step 8-14). The united output data is held in the register C 703 (at step 8-15). With this step, a second process including the function FI operating circuit 724 has been completed.

[0092] Next, in the selector C 713, the data held in the register C 703 is selected (at step 8-16). The selected data (2 × m bits) is divided into two m-bit data, and one m-bit data is output as an output data without any transformation. The other m-bit data is input to the function FI operating circuit 724 to be transformed. The transformed data is XORed bit by bit by the XOR circuit 723 with the other m-bit data, and the XORed result and the output m-bit data are united (at step 8-14). The united output data is held in the register C 703 (at step 8-15). With this step, a third process including the function FI

operating circuit 724 has been completed.

[0093] Next, in the selector C 713, the data held in the register C 703 is selected (at step 8-16), and the selected data is selected by the selector D 714 (at step 8-18). Then, it is detected to be an even-numbered stage (at step 8-19), the selected data is fed back, and is XORed bit by bit by the XOR circuit 721 with the data held in the register A 701 (at step 8-25). The output data from the XOR circuit A 721 is selected by the selector A 711 (at step 8-26), and is held in the register A 701 (at step 8-27). With this step, the data transformation process of the second stage terminates.

[0094] Hereinafter, data transformation process similar to the data transformation processes of the first stage and the second stage is repeated alternately a necessary number of times. MISTY performs up to a transformation process corresponding to the transformation process of an eighth stage.

[0095] Then, a process of step 8-28 is performed. At step 8-28, the above steps 8-3 through 8-12 are performed. First, in the selector C 713, the data held in the register A 701 is selected (at step 8-3). Next, the selected data is transformed by the function FL operating circuit 725 (at step 8-4), and the output data is selected by the selector D 714 (at step 8-5). Further, the selected data is selected by the selector A 711 (at step 8-6), and is held in the register A 701 (at step 8-7).

[0096] Next, in the selector C 713, the data held in the register B 702 is selected (at step 8-8). The selected data is transformed by the function FL operating circuit 725 (at step 8-9), the output data is selected by the selector D 714 (at step 8-10). Further, the selected data is selected by the selector B 712 (at step 8-11), and is held in the register B (at step 8-12).

[0097] Finally, the data held in the register A 701 and the register B 702 are output as an output data A 753 and an output data B 754 (at step 8-29).

[0098] According to this embodiment, the cipher processing apparatus does not need to include three function FI operating circuits and three XOR circuits even when the functions FO 511 through 514 of each stage has such a configuration as shown in Fig. 11. It is enough for the cipher processing apparatus to include only one function FI operating circuit and one XOR circuit, which enables to reduce a circuit scale. Further, the cipher processing apparatus does not need to include a plurality of circuits for the functions FL 501 through 504 even when the cipher algorithm has a configuration as shown in Fig. 10. It is enough for the cipher processing apparatus to include only one function FL operating circuit, which also enables to reduce a circuit scale.

[0099] In case of MISTY of this embodiment, a function used for the function FI and the function FL should be strong against cryptanalysis, so that the function has an extremely complex configuration. Hence, the reduction of the circuit scale according to the present invention is quite effective.

[0100] Further, as clearly understood by the above description of the embodiment, it is not always required to operate the registers A through C, and the selectors A through D. The process can be performed with these circuits operating only when required, which takes a great effect on saving electric power.

[0101] Accordingly, it is very effective to apply this invention to a small apparatus such as an IC card. The invention can be applied not only to the IC card, but also to a reader/writer for the IC card.

Embodiment 3.

[0102] Figs. 16 and 17 show general configurations of communication system of one embodiment of the present invention.

[0103] In Figs. 16 and 17, a reference numeral 91 shows a reader/writer, a reference numeral 92 shows an IC (integrated circuit) card, and 93 shows an IC of the IC card 92. The IC 93 includes configurational elements: a transmitter/receiver 94 for transmitting/receiving communication data; a CPU (central processing unit) 95 for controlling the apparatus; a memory 96 for storing data and program, etc.; and a cipher processing apparatus 97 for encrypting/decrypting a communication data. The IC 93 includes the transmitter/receiver 94, the CPU 95, the memory 96, and the cipher processing apparatus 97 as configurational elements.

[0104] The cipher processing apparatus described in the first or the second embodiment is applied to the cipher processing apparatus 97.

[0105] In this communication system, the encrypted data is transmitted. Namely, in the IC card 92, the transmitter/receiver 94 transmits data encrypted by the cipher processing apparatus 97 to the reader/writer 91. The transmitter/receiver 94 also receives data transmitted from the reader/writer 91, and the received data is decrypted by the cipher processing apparatus 97 to implement communication.

[0106] In this case, communication between the reader/writer 91 and the IC card 92 can be either connected or unconnected.

Industrial Applicability

[0107] As has been described, according to the invention, in the communication system using encrypted data, the circuit scale of the cipher processing apparatus can be reduced and the electric power can be saved.

[0108] Further, an IC card can be effectively configured by applying the cipher processing apparatus of the invention. The reduction of the circuit scale and the saving electric power has been performed in the IC card.

Claims

1. A cipher processing apparatus performing a first

data transformation process on an input data a plurality of times by a first operating circuit, wherein:

the first operating circuit comprises a loop processing circuit for performing a second data transformation process a plurality of times;
wherein the loop processing circuit comprises a second operating circuit, a data holding circuit, and a selecting circuit to form a processing loop;
wherein the second operating circuit performs the second data transformation process;
the data holding circuit tentatively holds the data on which the second data transformation process was performed; and
the selecting circuit selects one of to terminate and to continue the second data transformation process by the loop processing circuit.

2. The cipher processing apparatus of claim 1, wherein the second operating circuit comprises:

a data dividing circuit dividing data input to the second operating circuit into a first divided data and a second divided data;
a third operating circuit transforming the first divided data;
an XOR circuit XORing an output data from the third operating circuit with the second divided data bit by bit; and
a data uniting circuit uniting an output data from the XOR circuit and the second divided data.

3. The cipher processing apparatus of claim 1, wherein the selecting circuit inputs a data for the first data transformation process by the first operating circuit and a data held in the data holding circuit, and the selecting circuit selects the data held in the data holding circuit when a process by the loop processing circuit is to be continued.

4. The cipher processing apparatus of claim 3, wherein the selecting circuit selects the data for the first data transformation process by the first operating circuit when a process by the processing loop circuit starts.

5. The cipher processing apparatus of claim 4, further comprising:

a register A and a register B alternately holding the data for the first data transformation by the first operating circuit;
two XOR circuits XORing bit by bit the data on which the first data transformation was performed by the first operating circuit with the data held in the register A and with the data held in the register B, respectively;
a selector A and a selector B selecting one of the data on which the first data transformation was performed by a first operating unit and an XORed data by the XOR circuit to hold in the register A and the register B, respectively; and
wherein the selecting circuit alternately selects the register A and the register B to start the process of the loop processing circuit.

6. The cipher processing apparatus of claim 1, wherein the first operating circuit further performs a data transformation different from the second data transformation process for the data on which the second data transformation was performed by a processing loop unit to output a transformed data.

7. The cipher processing apparatus of claim 1, wherein the second operating circuit comprises:

m ($m \geq 1$) number of function operating circuits inputting identical data from the selecting circuit; and
a selector with m inputs and one output for inputting data operated by the m number of function operating circuits and selecting one of the input data.

8. The cipher processing apparatus of claim 2, further comprising:

a function operating unit transforming data output from the selecting circuit; and
a selector inputting data operated by the function operating unit and the data output from the selecting circuit, and outputting one of the data.

9. A cipher processing method performing a first data transformation for an input data a plurality of times by a first operating step, wherein:

the first operating step comprises a loop processing step performing a second data transformation at a plurality of times;
wherein the loop processing step comprises:
a second operating step performing the second data transformation;
a data holding step temporarily holding data on which the second data transformation was performed; and
a selecting step for selecting either of to terminate and to continue the second data transformation by the loop processing step.

10. The cipher processing method of claim 9, wherein the second operating step comprises:

a data dividing step dividing data input to the second operating step into a first divided data

and a second divided data;

a third operating step transforming the first divided data;

an XOR step XORing an output data from the third operating step with the second divided data bit by bit; and

a data uniting step uniting an output data from the XOR step and the second divided data.

11. An IC (integrated circuit) card communicating data with a reader/writer comprising:

a data receiving circuit receiving the data from the reader/writer;

a data transmitting circuit transmitting the data to the reader/writer; and

the cipher processing apparatus of claim 1 encrypting/decrypting the data.

12. An IC card communicating data with a reader/writer comprising:

a data receiving circuit receiving the data from the reader/writer;

a data transmitting circuit transmitting the data to the reader/writer; and

the cipher processing apparatus of claim 2 encrypting/decrypting the data.

Fig. 1

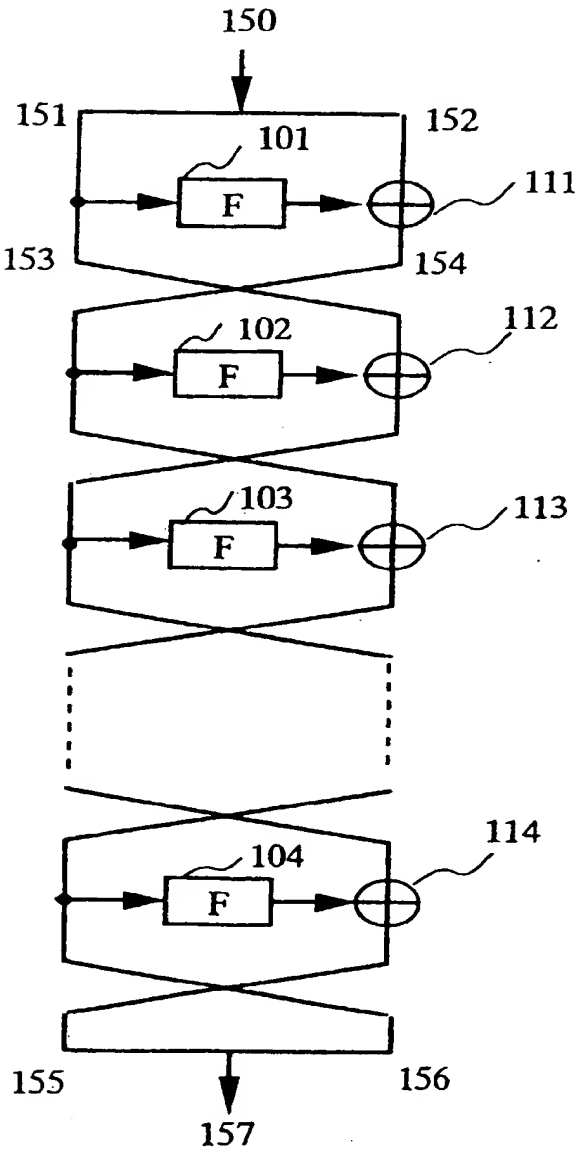


Fig.2

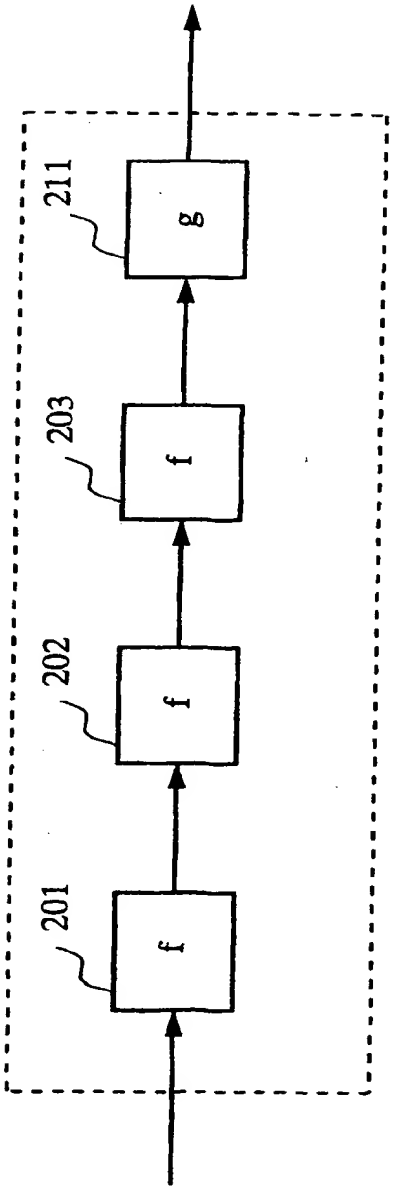


Fig. 3

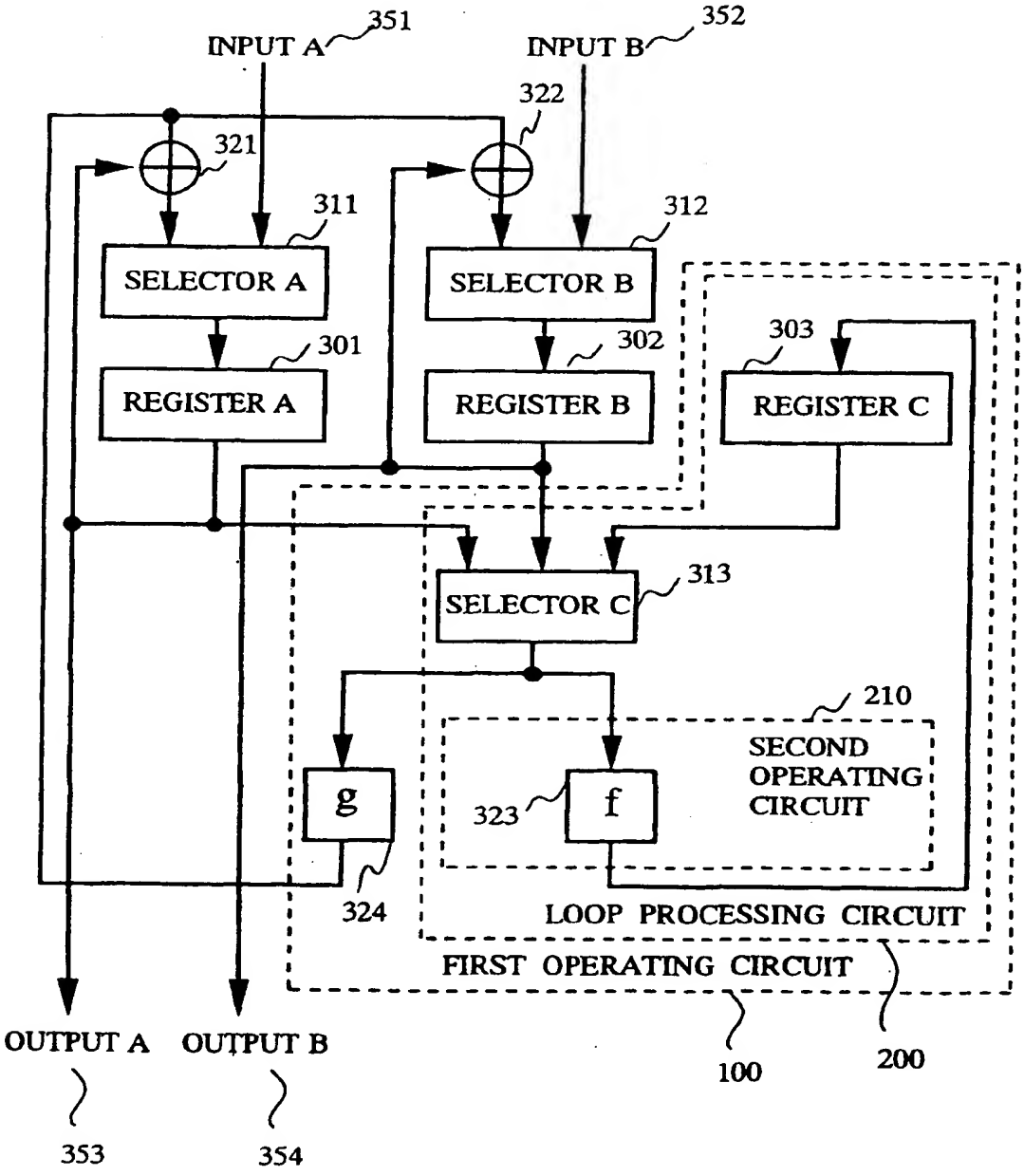


Fig. 4

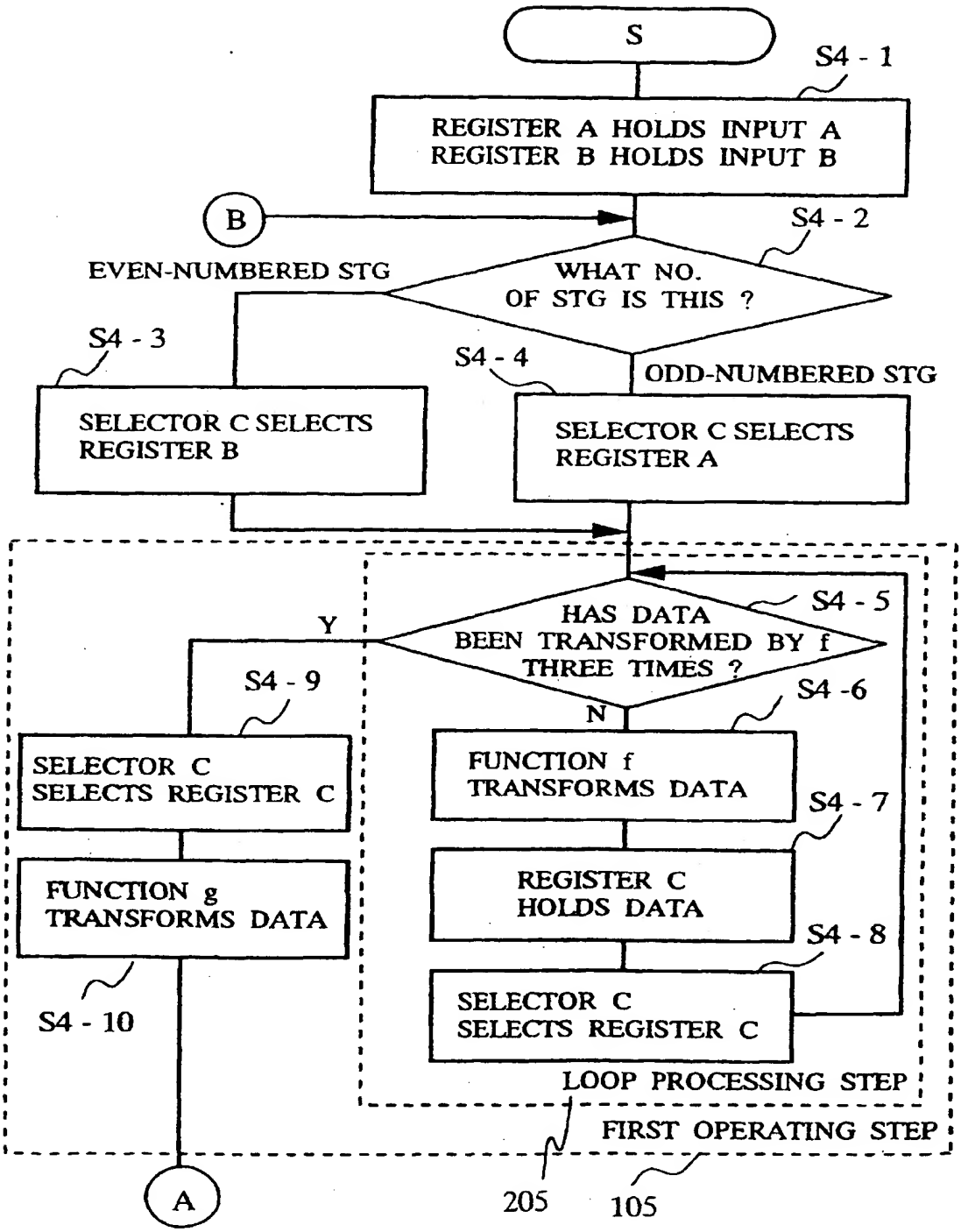


Fig. 5

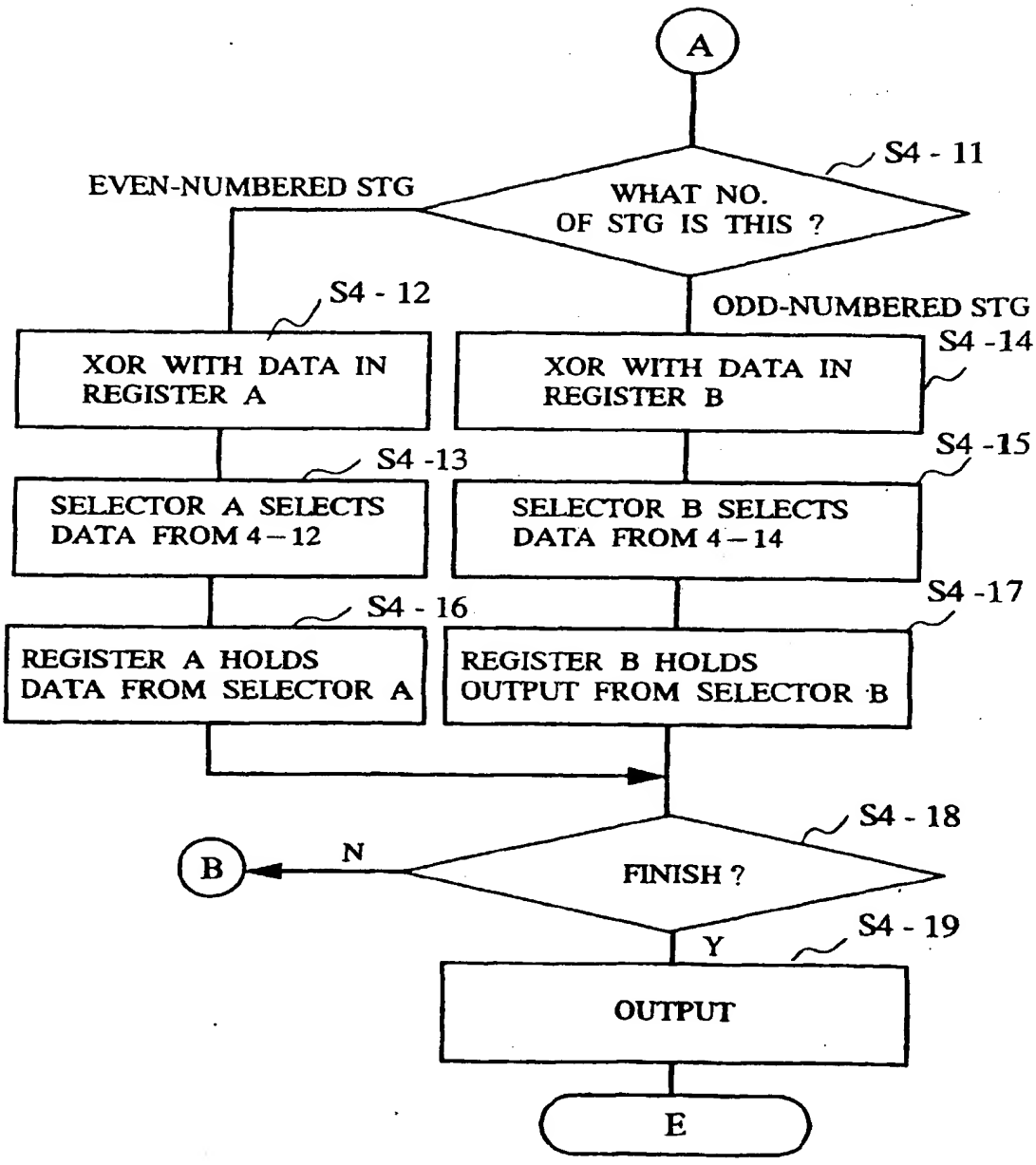


Fig.6

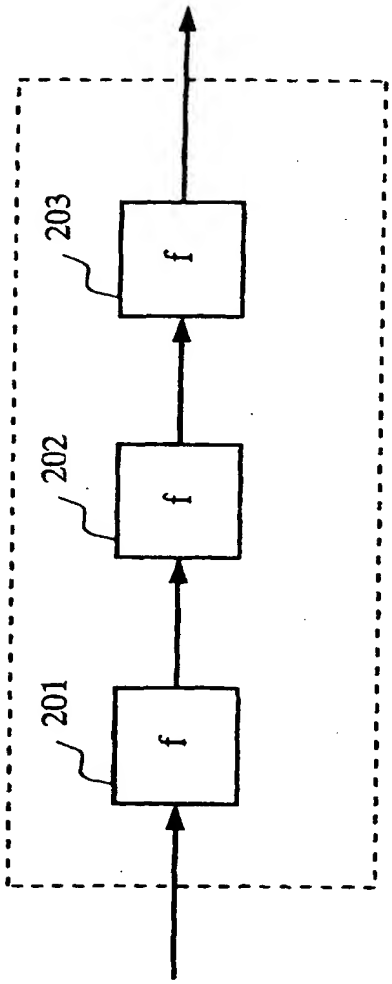


Fig. 7

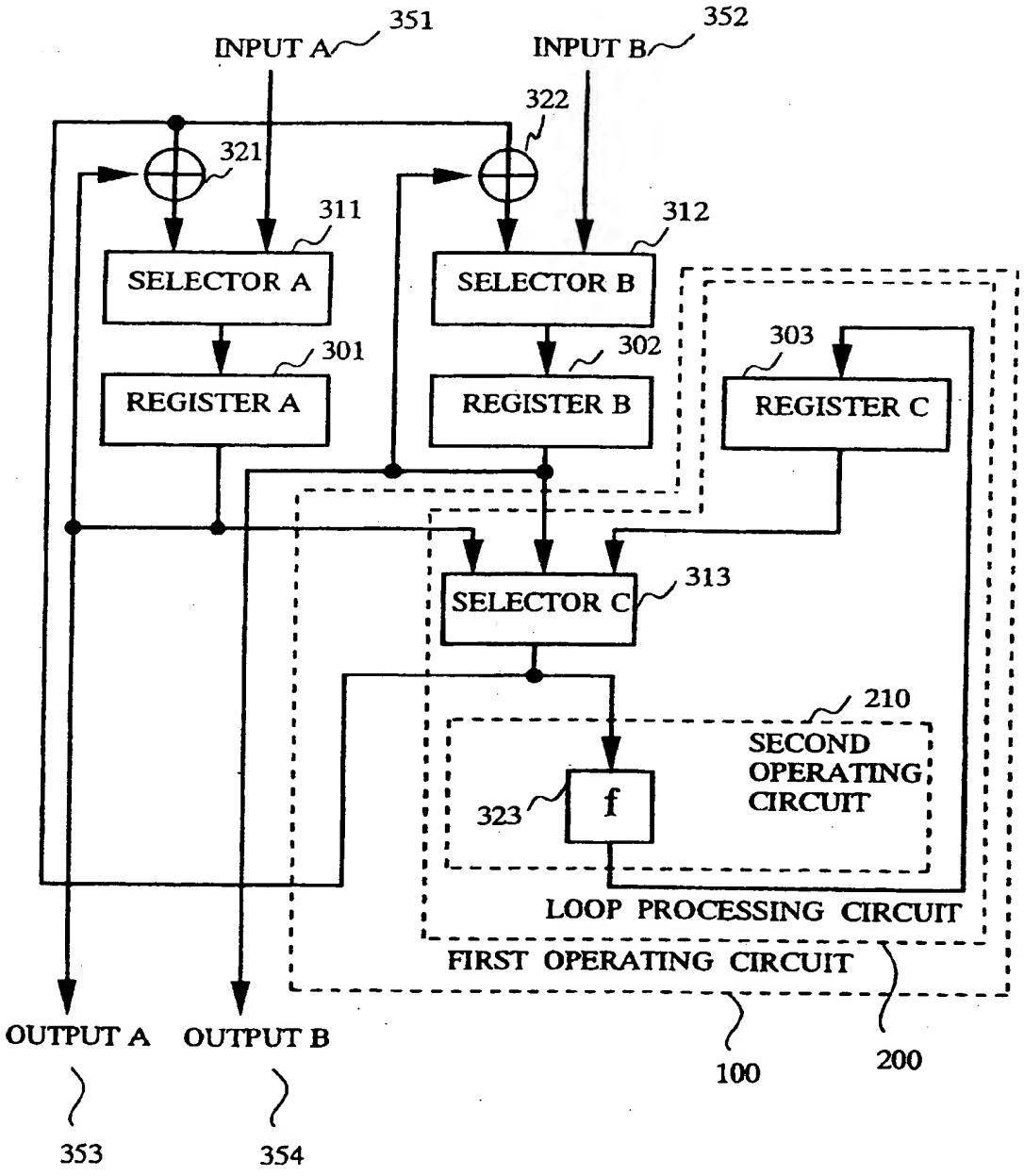


Fig.8

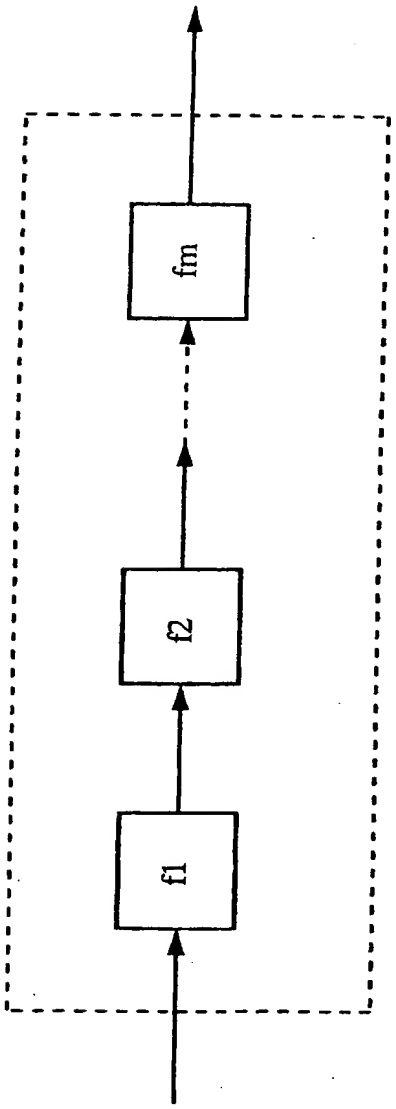


Fig. 9

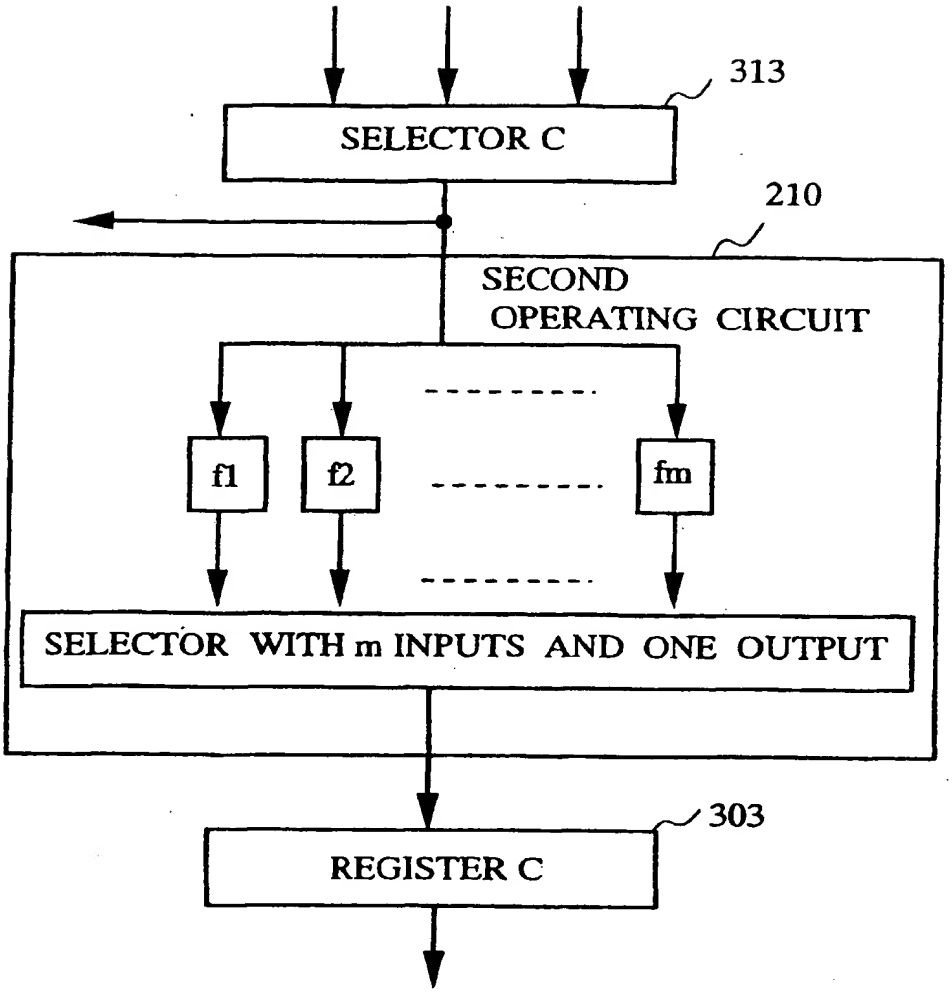


FIG. 10

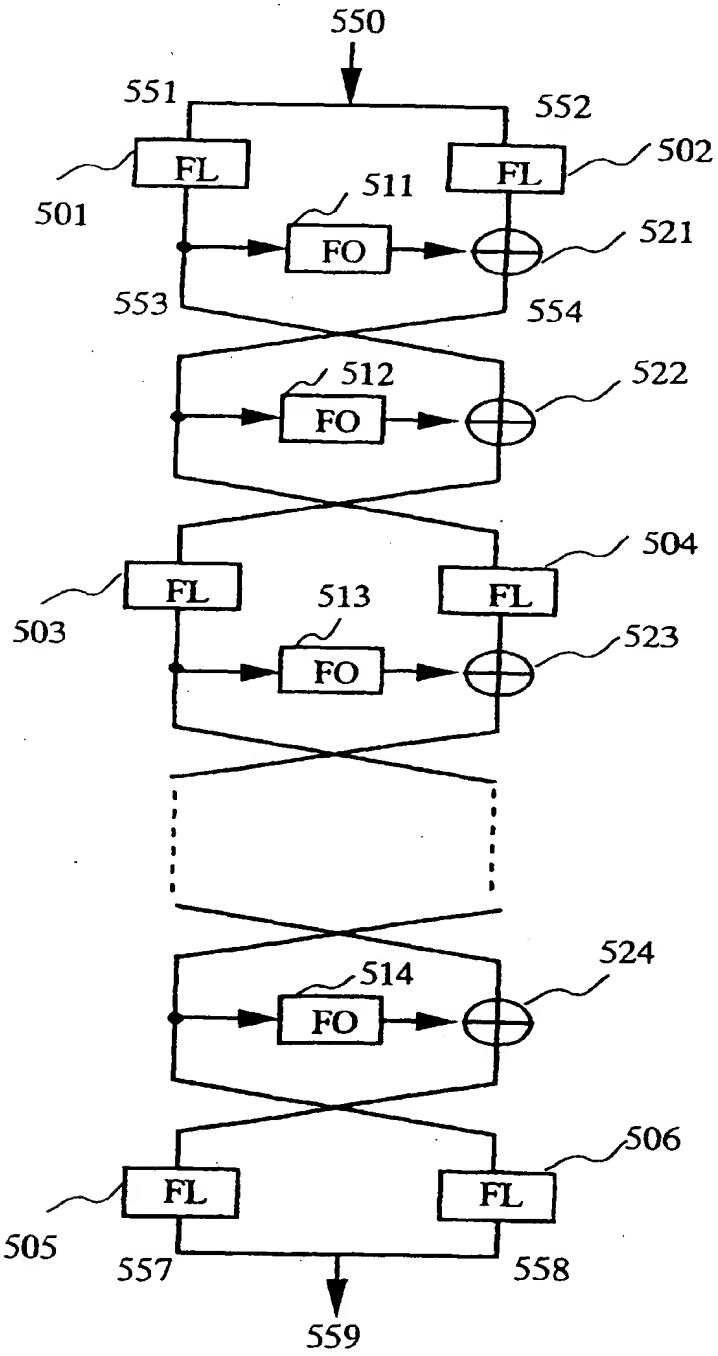


FIG. 11

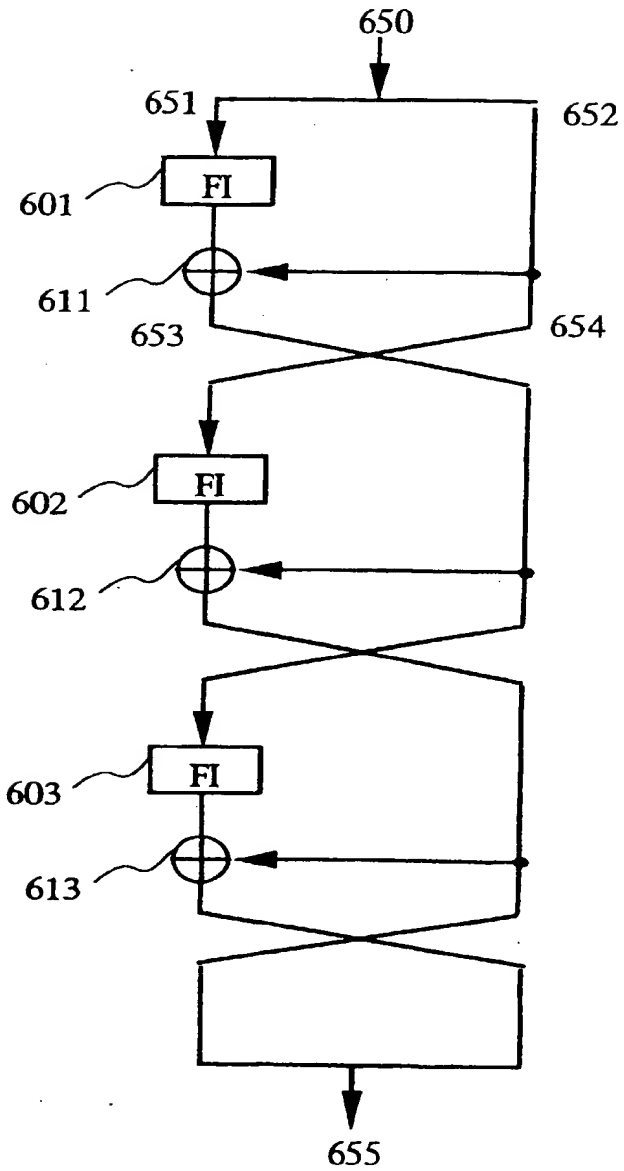


Fig. 12

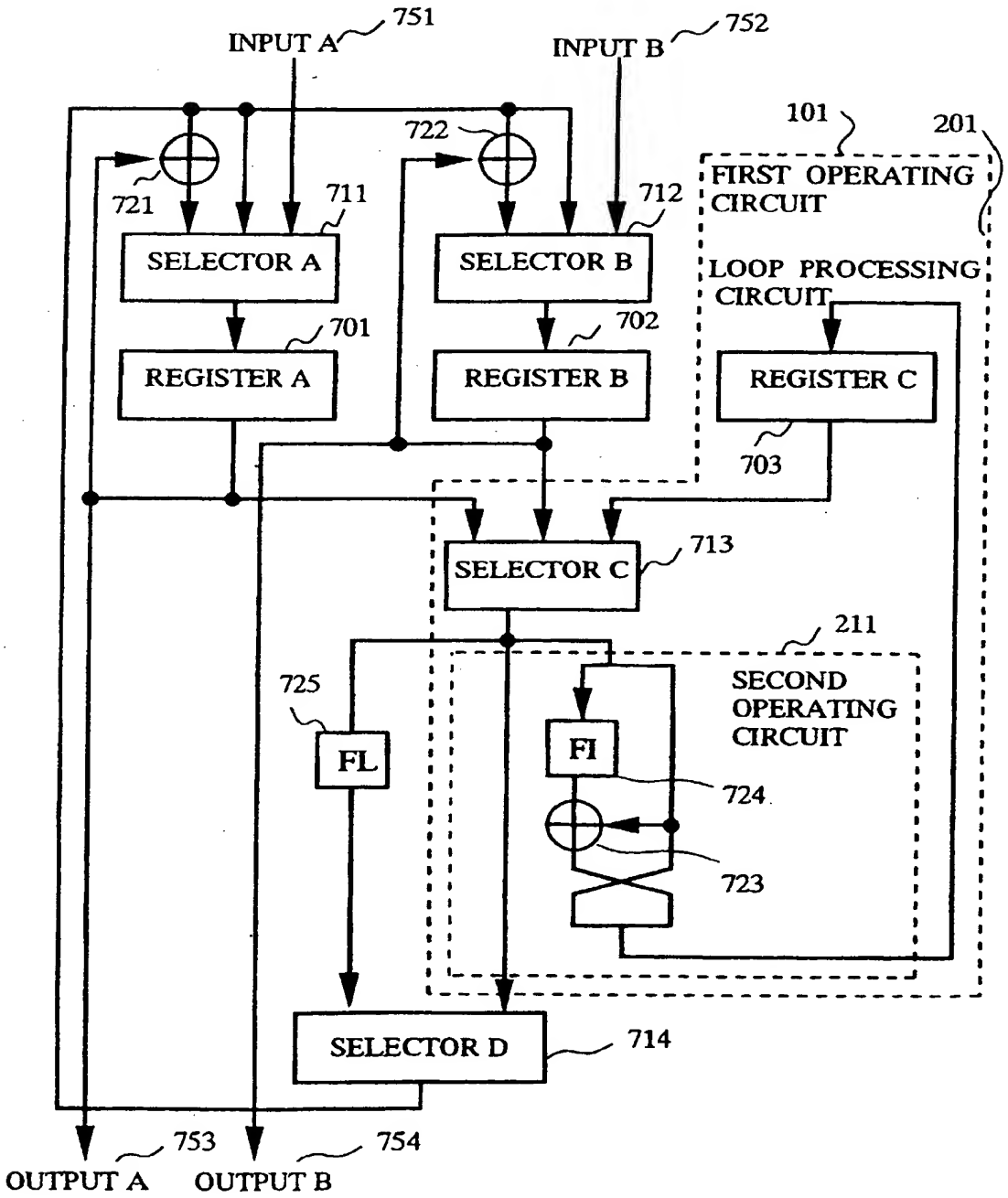


Fig. 13

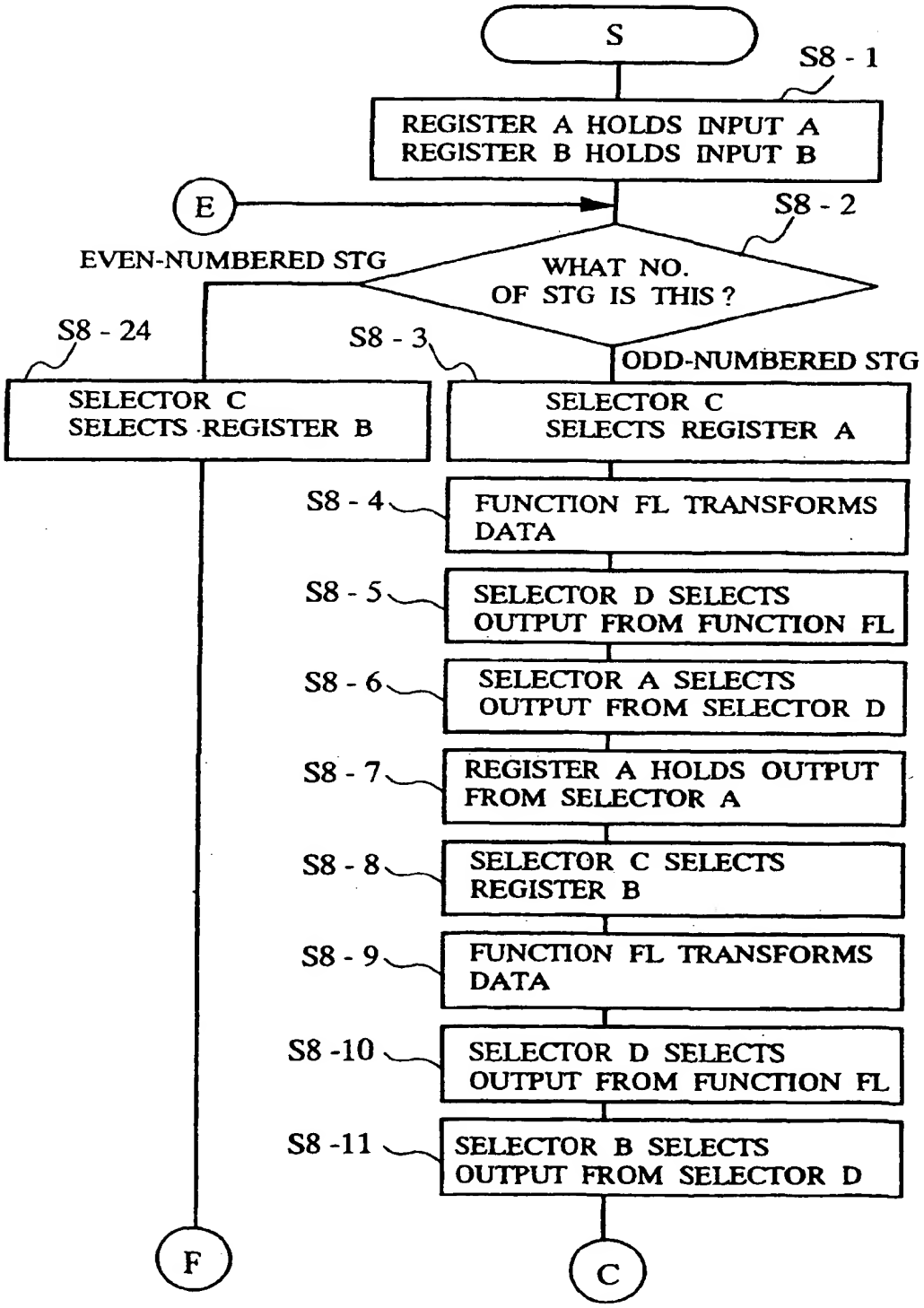


Fig.14

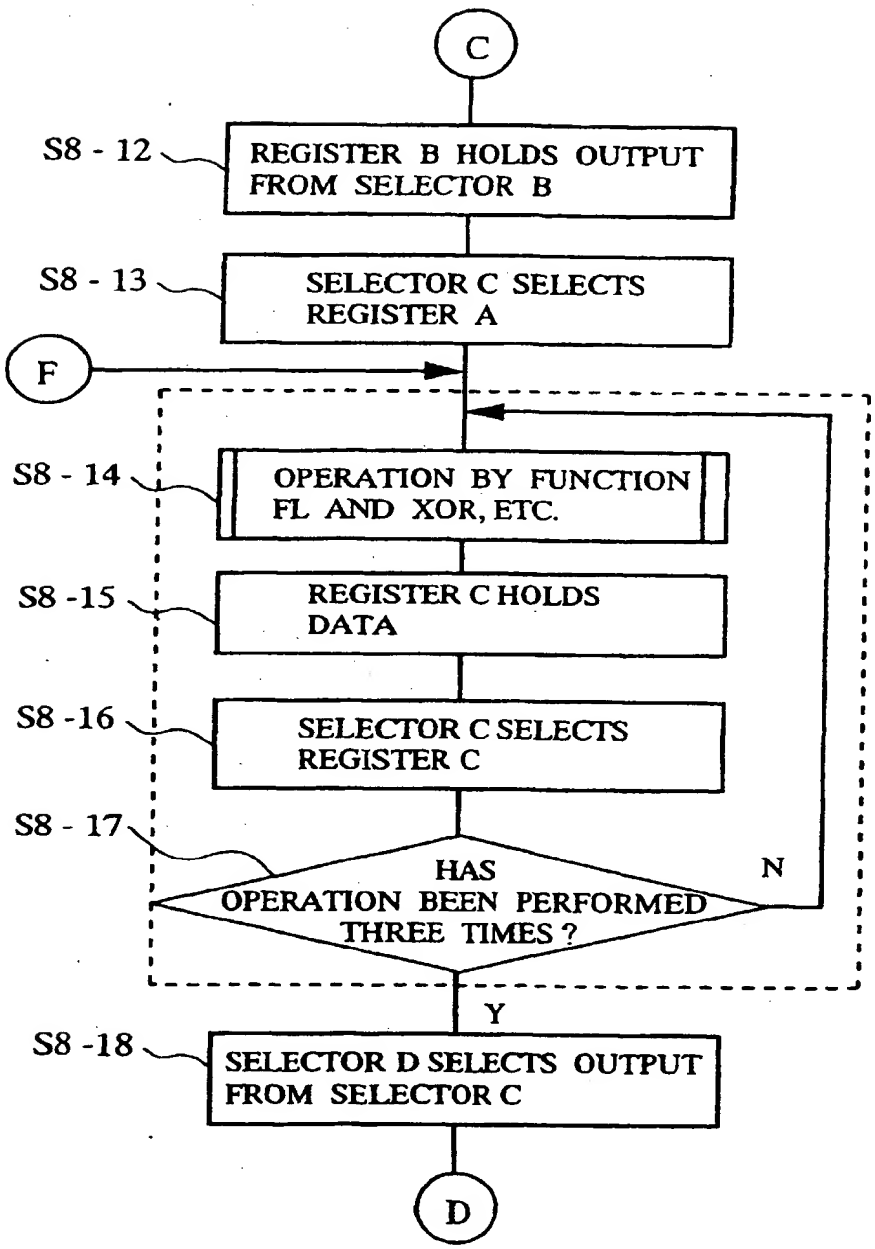


Fig. 15

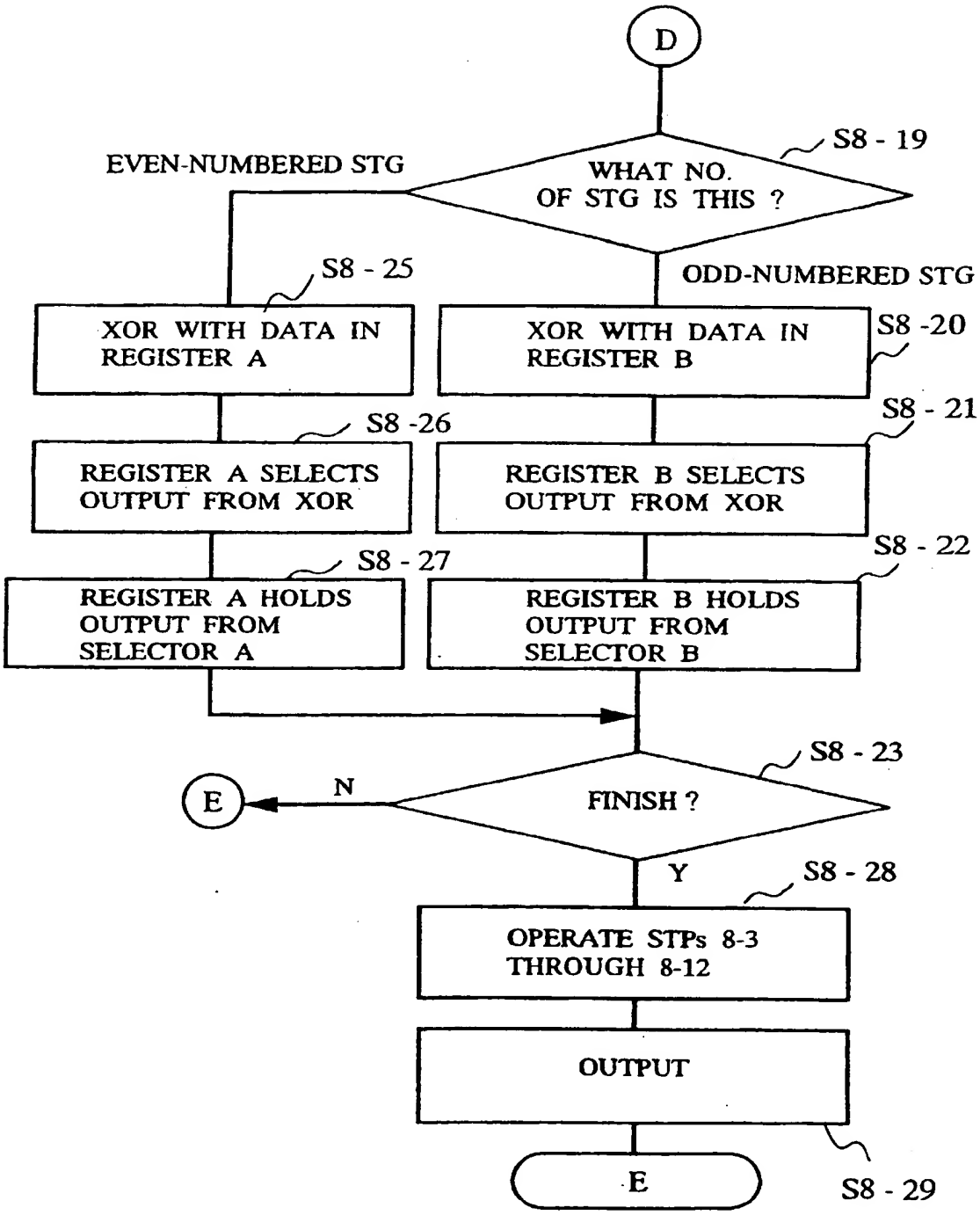


Fig.16

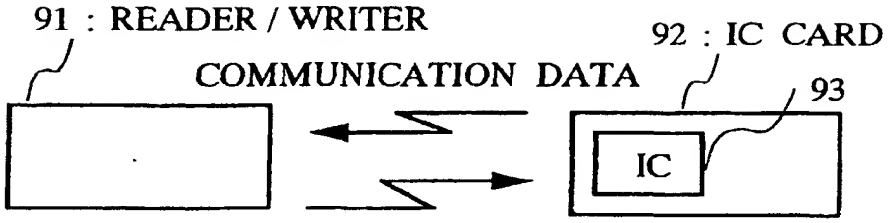


Fig.17

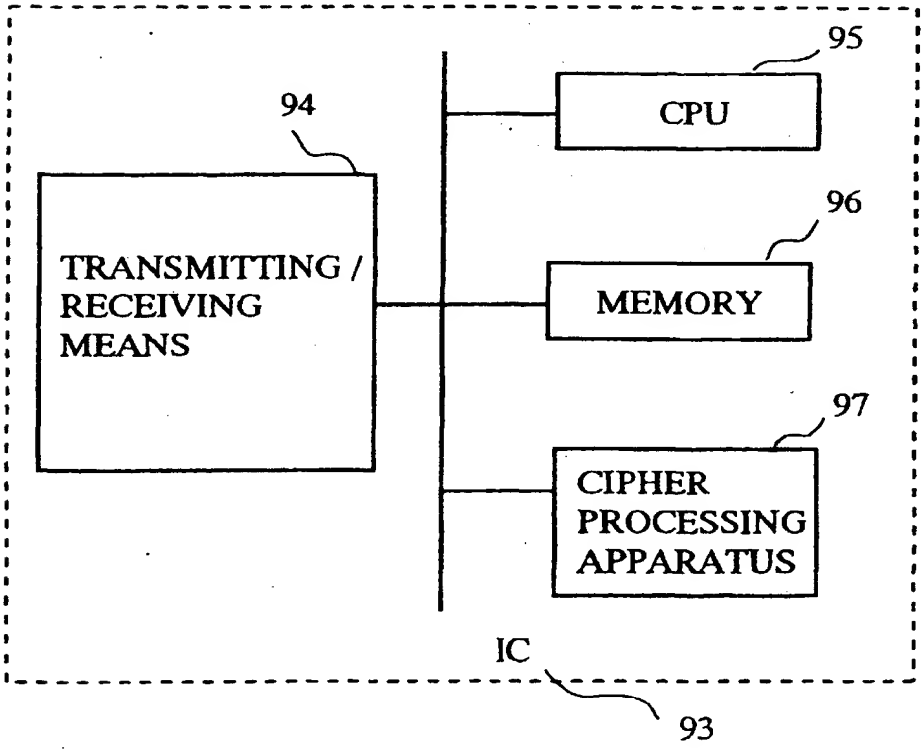


FIG. 18

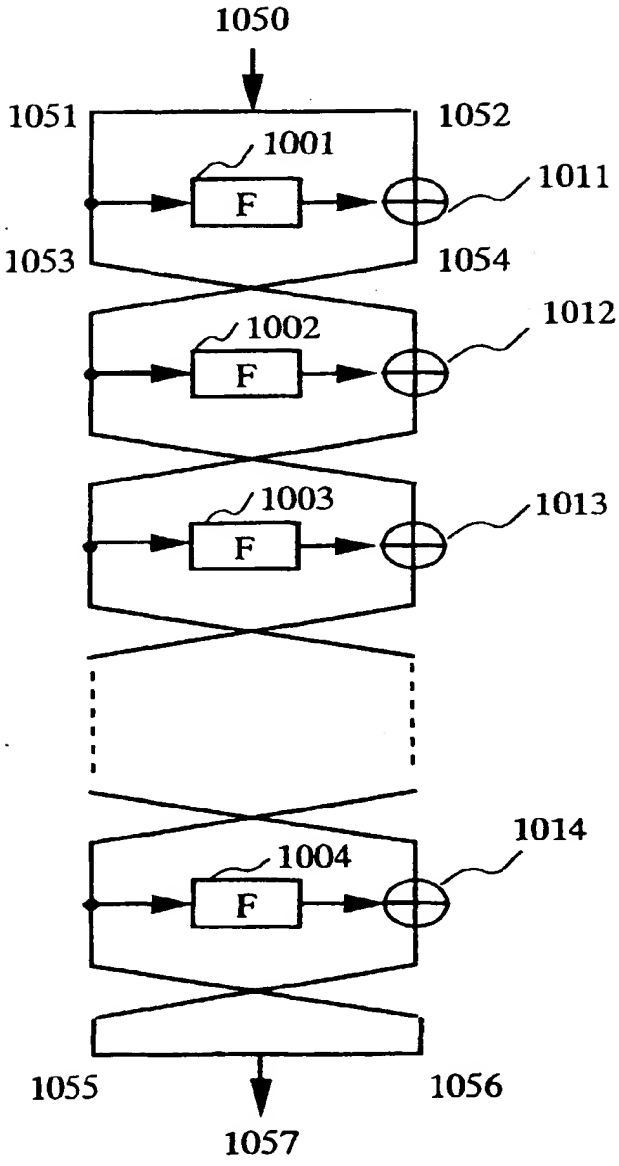
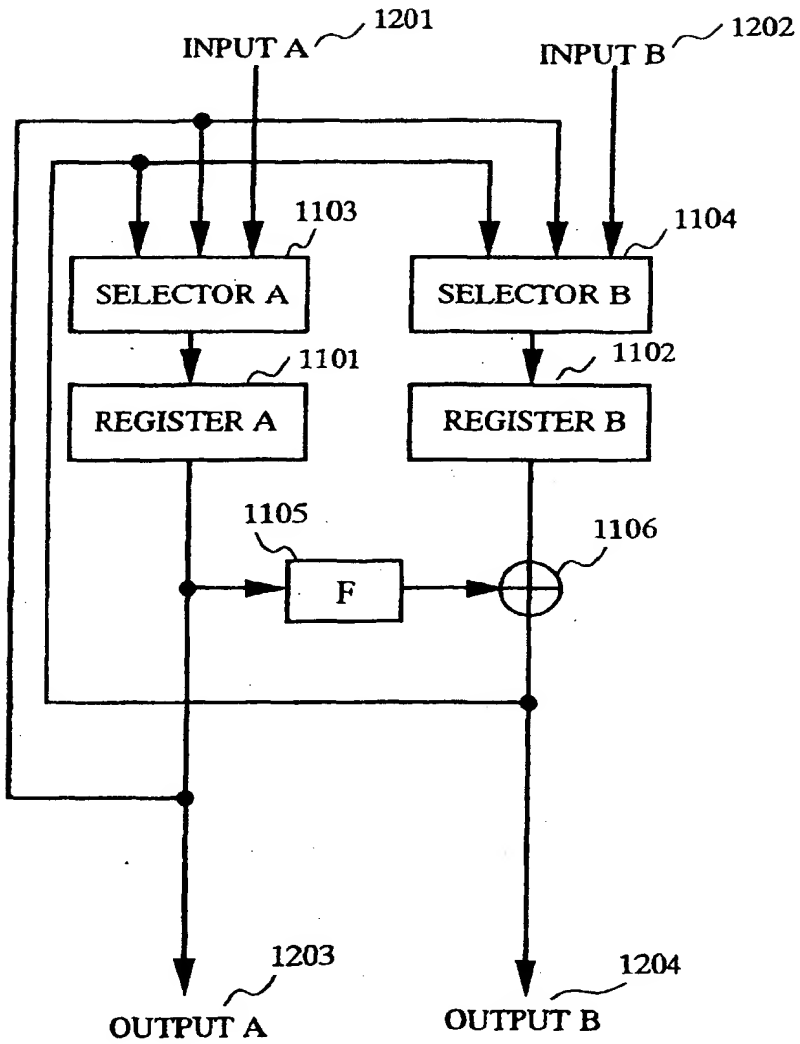


Fig. 19



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/01898

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G09C1/00, H04L9/06, G06K9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G09C1/00-5/00, H04L9/00-9/38, G06K9/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	WO, 97/09705, A1 (Mitsubishi Electric Corp.), March 13, 1997 (13. 03. 97), Particularly refer to Figs. 7, 12, 16 & AU, 9666293, A & NO, 9702052, A & EP, 790595, A1	1-6, 8-10 7, 11-12
Y	Mitsuru Matsui et al., "Practical Brock Cipher Having Provable Security for Difference Deciphering Method and Linear Deciphering Method (in Japanese)" Sympoisum on Cipher and Information Security, SCIS96, Information Security Research Special Comittiee of IEICE, January 1996, SCIS96-4C	1-12
Y	Mitsuru Matsui, "Block Cipher Algorithm MISTY (in Japanese)" Technical Research Report of IEICE, Vol. 96, No. 167, July 1996, p.35-48, (ISEC96-11)	1-12

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
July 16, 1998 (16. 07. 98)	July 28, 1998 (28. 07. 98)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210(second sheet)(July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP98/01898

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	Mitsuru Matsui, "New Structure of Block Ciphers with Provable Security against Differential and Linear Cryptanalysis", Lecture Notes in Computer Science, Vol. 1039, (1996), p.205-218	1-12
Y	H. Morita, M. Yamane, "Hardware Approach to Fast Encipherment Processing and Its Implementation", IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E74, No. 8, Aug. 1991, p.2143-2152 Particularly refer to Fig. 4	1-12
Y	Hassei Akiyama, "Cipher Processing Hardware (in Japanese)", Journal of the Information Processing Society of Japan, Vol. 25, No. 6, 1984, p.566-574 Particularly refer to Fig. 1 ; page 567	1-12
Y	JP, 4-365240, A (Mitsubishi Electric Corp.), December 17, 1992 (17. 12. 92), Particularly refer to Fig. 4 & EP, 518315, A2 & US, 5261003, A & US, 5488661, A	7
Y	JP, 4-256195, A (Toshiba Corp.), September 10, 1992 (10. 09. 92) & EP, 500244, A2	11, 12
Y	JP, 3-64788, A (N.V. Philips' Gloeilampenfabrieken), March 20, 1991 (20. 03. 91) & EP, 410516, A & FR, 2650458, A & US, 5168521, A	11, 12

Form PCT/ISA/210(continuation of second sheet)(July 1992)